UNITED STATES DISTRICT COURT

for the

IN THE MATTER OF THE SEARCH O

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Information associated with Charter Account 8260130364407299 that is stored at premises owned, maintained, controlled, or operated by Charter Communications, Inc., a company headquartered at 400 Atlantic Street, Stamford, CT 06901

Case No. 22-875M(NJ)

Matter No.: 2021R00295

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A.

located in the _____ District of _____, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 245 and 18 U.S.C. § 875(c)	See attached affidavit

The application is based on these facts:

See attached affidavit.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

SA Eric Burns, FBI
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone *(specify reliable electronic means)*.

Date: May 11, 2022

Judge's signature

City and state: Milwaukee, WI.

Honrable Nancy Joseph, Magistrate Judge
Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF WISCONSIN

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH CHARTER ACCOUNT 8260130364407299 THAT IS STORED AT PREMISES CONTROLLED BY CHARTER COMMUNICATIONS, INC.	Case No. 22-875M(NJ)

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR SEARCH WARRANT

I, Eric Burns, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for search warrants under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Charter Communications, Inc. ("Charter," also d/b/a "Spectrum") to disclose to the United States records and other information associated with the above-listed Charter account that is stored at premises owned, maintained, controlled, or operated by Charter, a company headquartered at 400 Atlantic Street, Stamford, CT 06901. The information to be disclosed by Charter and searched by the United States is described in the following paragraphs and in Attachments A and B.

2. I have been a Special Agent with the Federal Bureau of Investigation ("FBI") since November 2009. I am currently assigned to an FBI squad which investigates financial crimes, civil rights crimes, and public corruption crimes. During my tenure with the FBI, I have participated in investigations involving threats made using electronic media, to include threats made via email. I have participated in all aspects of investigations including executing search warrants involving, among other things, the search and seizure of computers, computer equipment, software, and electronically stored information.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show simply that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on the facts as set forth in this affidavit, there is probable cause to believe that the information described in Attachment A contains evidence, instrumentalities, and/or fruits of violations of Title 18, U.S.C. § 245 and 18 U.S.C. § 875(c) (collectively, "Subject Offenses"), as described in Attachment B.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

6. The FBI is investigating threats made over interstate communications, specifically an electronic message threat sent to Claire Woodall-Vogg, an election official who worked during the relevant period with the Election Commission of the City of Milwaukee, Wisconsin (hereinafter "VICTIM-1"), which included language indicating a desire to harm VICTIM-1.

7. On November 4, 2020, at approximately 4:07 am, CDT, VICTIM-1 received an email to VICTIM-1's government email account from an individual serving as Wisconsin's state lead for The Elections Group, an elections consulting partnership (hereinafter "INDIVIDUAL-1"), with the subject line, "drama." The email said, "Damn, Claire, you have a flair for drama, delivering just the margin needed at 3:00 am. I bet you had those votes counted at midnight, and

just wanted to keep the world waiting!" VICTIM-1 responded to INDIVIDUAL-1 approximately 10 minutes later, "Lol. I just wanted to wait to say I had been awake for a full 24 hours!"

8. On or about July 27, 2021, and on or about July 31, 2021, respectively, the websites Wisconsin Spotlight and Gateway Pundit published a copy of the email exchange between INDIVIDUAL-1 and VICTIM-1 on their websites. As a result of the email exchange being published, between July 31, 2021, and August 2, 2021, VICTIM-1 received at least 150 emails regarding her participation in perceived fraudulent activity surrounding the outcome of the 2020 U.S. Presidential Election. Several of the emails VICTIM-1 received included language indicating a desire to harm VICTIM-1.

9. On Tuesday, September 14, 2021, at 1:23 am, CDT, VICTIM-1 received an email from "thetower.062020@protonmail.com" to her personal email account. The subject line of the email sent to VICTIM-1 from thetower.062020@protonmail.com was "Hello Marxist Bitch." The body of the email said, "Thankfully the The Gateway Pundit brought your betrayal of Wisconsin and America to my attention, Fox News and Breitbart don't do shit these days. I hope you know there are consequences for your actions. I know a lot of information about you. I will have to think about what comes next. Sent with ProtonMail Secure Email."

10. All of the emails VICTIM-1 received between July 31, 2021, and August 2, 2021, regarding VICTIM-1's participation in perceived fraudulent activity surrounding the outcome of the 2020 U.S. Presidential Election were sent either to VICTIM-1's government email account or the City of Milwaukee Election Commission public-facing email account. The email sent to VICTIM-1 from thetower.062020@protonmail.com on September 14, 2021, was the first such email VICTIM-1 received to her personal email account. VICTIM-1's personal email address was not easily accessible to a member of the public through use of search engines such as Google.

11. According to information received from Proton Technologies AG on October 1, 2021, through the FBI Legat process, thetower.062020@protonmail.com listed a recovery email address of "swordofthe.evening@pm.me." Also according to information received from Proton Technologies AG on October 1, 2021, swordofthe.evening@pm.me had multiple email aliases,[1] to include email alias addresses "carson.king@pm.me" and "0.carson@protonmail.com."

12. According to information received by subpoena from Twitter on October 5, 2021, the thetower.062020@protonmail.com email address was used to create Twitter account "@king_sobieski" on March 26, 2021. However, in April 2021, the account was suspended for violating Twitter's Rules and Terms of Service.

13. According to information received by subpoena from Twitter on October 15, 2021, the swordofthe.evening@pm.me email address was used to create Twitter account "@agentsmith2021" on June 4, 2020, and listed telephone number 972-674-8260 as a contact number. Furthermore, the 0.carson@protonmail.com email address was used to create Twitter account "@777focusedspark" on July 22, 2017. The @777focusedspark Twitter account was logged into as recently as October 2021, through IP address 76.187.202.157, which resolves back to Dallas, Texas.

14. On November 5, 2020, Twitter account @agentsmith2021 posted a Tweet referencing alleged election fraud during the 2020 U.S. Presidential Election.

15. According to information received by subpoena from Charter on December 10, 2021, from June 11, 2021 to October 21, 2021, IP address 76.187.202.157 was assigned to Charter

[1] An email alias is an additional email address for an email account. A single user account can have multiple aliases, which either the same domain or with a different domain.

account 8260130364407299 (the "Account"). The Account is registered to Carson King ("KING") with a service and billing address located in Dallas, Texas. Furthermore, the Account listed carson.king@pm.me and 972-647-8260 as its email address and telephone number, respectively.

16. Also according to information received by subpoena from Charter on December 10, 2021, the Account was assigned the following IP addresses during the following time periods:

a. IP address 76.187.208.110 from March 23, 2021, to June 12, 2021.

b. IP address 76.187.193.0 from September 11, 2020, to March 23, 2021.

17. Throughout this investigation, I have received information for several online accounts maintained by KING wherein the online activity associated with the accounts coincide with the IP addresses assigned to the Account during the time periods as stated in Paragraphs 15 and 16 above. For example:

a. According to information received from Google by subpoena on October 20, 2021, Google Account 842495047147 is registered to email address carson.cccxcv@gmail.com and is subscribed to by KING with recovery email address carson.king@pm.me. A review of the account's login activity revealed the following:

i. Between June 11, 2021 and October 13, 2021, the account was frequently logged into from IP address 76.187.202.157.[2]

[2] There was a gap of login activity from August 21, 2021, to September 19, 2021, but the subpoena return does not provide transactional information with respect to any logouts. Given my training and experience, I understand that it is plausible that the Google Account was logged into for the entirety of that time period.

ii. Between April 6, 2021, and June 3, 2021, the account was frequently logged into from IP address 76.187.208.110.

iii. Between January 21, 2021, and March 15, 2021, the account was occasionally logged into from IP address 76.187.193.0.

b. According to information received from Coinbase by subpoena on October 15, 2021, KING opened a Coinbase account on June 29, 2019. A review of the account's IP activity revealed the following:

i. Between November 23, 2020, and March 22, 2021, there was frequent activity associated with the account, such as an account login, from IP address 76.187.193.0.

ii. Between March 30, 2021, and May 12, 2021, there was frequent activity associated with the account from IP address 76.187.208.110.

iii. Between June 11, 2021, and September 28, 2021, there was frequent activity associated with the account from IP address 76.187.202.157.

c. According to information received from Amazon by subpoena on November 24, 2021, KING has maintained an Amazon account since May 20, 2010. A review of the account's order history revealed the following:

i. Between September 13, 2020, and March 14, 2021, KING placed approximately 208 orders, the majority of which were placed from IP address 76.187.193.0.

ii. Between April 1, 2021, and June 11, 2021, KING placed approximately 90 orders, the majority of which were placed from IP address 76.187.208.110.

iii. Between June 16, 2021, and October, 3, 2021, KING placed approximately 82 orders, the majority of which were placed from IP address 76.187.202.157.

d. According to information received from Spotify by subpoena on October 26, 2021, KING has maintained a Spotify account since April 25, 2013. A review of the account's IP activity related to Spotify's streaming service revealed the following:

i. Between September 11, 2020, and December 25, 2020, there was frequent activity associated with the account from IP address 76.187.193.0.

ii. Between December 26, 2020, and June 10, 2021, there was no activity associated with the account.[3]

iii. Between June 11, 2021, and October 16, 2021, there was frequent activity associated with the account from IP address 76.187.202.157.

[3] According to information received from Spotify, KING paid for Spotify's streaming service via PayPal. According to information received from PayPal by subpoena on October 25, 2021, KING had recurring monthly transactions for "Spotify USA Inc," but there were no transactions between December 2020 and May 2021, meaning KING likely did not utilize Spotify's service during that time period.

e. According to information received from PayPal by subpoena on October 25, 2021, KING currently maintains two PayPal accounts. A review of the accounts IP activity revealed the following:

i. Between September 25, 2020, and March 5, 2021, the accounts had frequent activity associated with IP address 76.187.193.0.[4]

ii. Between March 25, 2021, and June 10, 2021, one of the accounts had frequent IP activity associated with IP address 76.187.208.110.

iii. Between June 11, 2021, and September 20, 2021, one of the accounts had frequent IP activity associated with IP address 76.187.202.157.

f. According to information received from Apple by subpoena on November 9, 2021, KING created an Apple iCloud account on June 20, 2020. A review of the account's IP activity revealed multiple logins on August 2, 2021, from IP address 76.187.202.157.

18. According to Charter's Privacy Policy, available at https://www.spectrum.com/policies/privacy-policy, Charter collects certain personal identifying information from subscribers when they register for an account, such as: the subscriber's full name, physical address, telephone numbers, email addresses, and payment information.

19. Charter's Privacy Policy also identifies information that Charter may collect from subscribers relating to their use of Charter's services and products, including: device identifiers,

[4] One of the accounts had no IP activity after October 20, 2020, likely indicating KING no longer uses the account, even though it remains open.

network traffic data, performance and support data, Internet usage information (including information about websites visited), IP addresses, call records, user settings and preferences. Charter may also retain voicemail, email, and other content based on a subscriber's use of its phone, email, and cloud storage services.

20. In my training and experience, evidence of who was using the Account and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

21. Based on my training and experience, it is common for individuals who engage in criminal activities, such as stalking, to use the Internet to prepare for, in furtherance of, and to obfuscate their operations. Information maintained by Charter, including network traffic data and Internet usage information, may include evidence relating to the identification of VICTIM-1's personal e-mail address, the use of ProtonMail to send the threat, and the use of VPN and other anonymity services.

22. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (*e.g.*, accessing the online material referenced in the threat), or consciousness of guilt (*e.g.*, deleting account information or use of anonymization services in an effort to conceal evidence from law enforcement).

23. In some cases, account users will communicate directly with a provider about issues relating to their account, such as technical problems, billing inquiries, or complaints from other users. Providers typically retain records about such communications, including records of contacts

between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications.

24. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Charter can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, network traffic data, internet usage information, email, and voicemail may be evidence of who used or controlled the account at a relevant time, and device identifiers and IP addresses can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

25. Therefore, Charter's servers are likely to contain records, communications, and other information concerning the Account. In my training and experience, such information may constitute evidence of the crimes under investigation, including information that can be used to identify the user of the Account.

26. On March 29, 2022, a preservation request under 18 U.S.C. § 2703(f) was sent to Charter regarding Charter account 8260130364407299.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

27. I anticipate executing this warrant under the Electronic Communications Privacy Act, specifically 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Charter to disclose to the government copies of the records and other information (not including the content of communications) particularly described in Section I of Attachment B.

Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

28. Based on the foregoing, I request that the Court issue the proposed search warrant.

29. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

30. The government will execute this warrant by serving the warrant on Charter. Because the warrant will be served on Charter, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with Charter Account 8260130364407299 that is stored at premises owned, maintained, controlled, or operated by Charter Communications, Inc., a company headquartered at 400 Atlantic Street, Stamford, CT 06901.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by the provider

To the extent that the information described in Attachment A is within the possession, custody, or control of Charter Communications, Inc. ("Charter," also d/b/a "Spectrum"), regardless of whether such information is located within or outside of the United States, and including any messages, records, files, logs, or information that have been deleted but are still available to Charter, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Charter is required to disclose the following information to the government for each account or identifier listed in Attachment A ("the Account"):

A. All business records and subscriber information, in any form kept, pertaining to the Account, including:

1. Identity and contact information (past and current), including full name, e-mail addresses, physical address, date of birth, phone numbers, gender, and other personal identifiers;

2. All usernames (past and current) and the date and time each username was active, all associated accounts (including those linked by machine cookie), and all records or other information about connections with other Charter or third-party products, services, websites, or apps;

3. Length of service (including start date), types of services utilized, purchases, and means and sources of payment (including any credit card or bank account number) and billing records;

4. Devices used to login to or access the Account, including all device identifiers, attributes, user agent strings, and information about networks and connections, cookies, operating systems, and apps and web browsers;

5. All advertising information, including advertising IDs, ad activity, and ad topic preferences;

6. Internet Protocol ("IP") addresses used to create, login, and use the Account, including associated dates, times, and port numbers, **from July 1, 2021, to the present;**

7. Privacy and account settings, including change history; and

8. Communications between Charter and any person regarding the Account, including contacts with support services and records of actions taken; and

B. All transactional and other records associated with the Account **from July 1, 2021, to the present**, including network traffic data, Internet usage information (including browsing history) and DNS data, local and long distance telephone connection records (including records of text messages sent and received), and IP logs or other records of session times and durations.

The Provider is hereby ordered to disclose the above information to the government within 14 days of service of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence and instrumentalities of violations of 18 U.S.C. § 245 and 18 U.S.C. § 875(c), and occurring after November 1, 2020, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

A. Records and information relating to VICTIM-1, VICTIM-1's personal email address, and/or the Election Commission of the City of Milwaukee, Wisconsin, including any communications with associates, organizations, or others that may contain VICTIM-1's personal information and/or referencing VICTIM-1;

B. Records and information relating threats, harassment, or intimidation by the subscriber, and/or targets or potential targets of threats, harassment, or intimidation by the subscriber;

C. The identity of the person(s) who created or used the Account, including records that help reveal the whereabouts of such person(s);

D. Evidence indicating how and when the Account was accessed or used, to determine the chronological and geographic context of Account access, use and events relating to the crime under investigation and the Account subscriber;

E. Any records pertaining to the means and source of payment for services (including any credit card or bank account number or digital money transfer account information);

F. Evidence indicating the subscriber's state of mind as it relates to the crime under investigation; and

G. Evidence that may identify any co-conspirators or aiders and abettors, including records that help reveal their whereabouts.

This warrant authorizes a review of electronically stored information, communications, and other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* Information associated with Charter Account 8260130364407299 that is stored at premises owned, maintained, controlled, or operated by Charter Communications, Inc., a company headquartered at 400 Atlantic Street, Stamford, CT 06901	)	Case No. 22-875M(NJ) **Matter No.: 2021R00295**

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the _____ District of _____
(identify the person or describe the property to be searched and give its location):

See Attachment A.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See Attachment B.

YOU ARE COMMANDED to execute this warrant on or before May 25, 2022 *(not to exceed 14 days)*
❒ in the daytime 6:00 a.m. to 10:00 p.m. ☒ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Honorable Nancy Joseph.
(United States Magistrate Judge)

❒ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*
❒ for _____ days *(not to exceed 30)* ❒ until, the facts justifying, the later specific date of _____.

Date and time issued: May 11, 2022 @ 12:46 p.m.

Nancy Joseph
Judge's signature

City and state: Milwaukee, WI. Honorable Nancy Joseph, Magistrate Judge
Printed name and title

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name(s) of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with Charter Account 8260130364407299 that is stored at premises owned, maintained, controlled, or operated by Charter Communications, Inc., a company headquartered at 400 Atlantic Street, Stamford, CT 06901.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by the provider

To the extent that the information described in Attachment A is within the possession, custody, or control of Charter Communications, Inc. ("Charter," also d/b/a "Spectrum"), regardless of whether such information is located within or outside of the United States, and including any messages, records, files, logs, or information that have been deleted but are still available to Charter, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Charter is required to disclose the following information to the government for each account or identifier listed in Attachment A ("the Account"):

A. All business records and subscriber information, in any form kept, pertaining to the Account, including:

1. Identity and contact information (past and current), including full name, e-mail addresses, physical address, date of birth, phone numbers, gender, and other personal identifiers;

2. All usernames (past and current) and the date and time each username was active, all associated accounts (including those linked by machine cookie), and all records or other information about connections with other Charter or third-party products, services, websites, or apps;

3. Length of service (including start date), types of services utilized, purchases, and means and sources of payment (including any credit card or bank account number) and billing records;

4. Devices used to login to or access the Account, including all device identifiers, attributes, user agent strings, and information about networks and connections, cookies, operating systems, and apps and web browsers;

5. All advertising information, including advertising IDs, ad activity, and ad topic preferences;

6. Internet Protocol ("IP") addresses used to create, login, and use the Account, including associated dates, times, and port numbers, **from July 1, 2021, to the present;**

7. Privacy and account settings, including change history; and

8. Communications between Charter and any person regarding the Account, including contacts with support services and records of actions taken; and

B. All transactional and other records associated with the Account **from July 1, 2021, to the present**, including network traffic data, Internet usage information (including browsing history) and DNS data, local and long distance telephone connection records (including records of text messages sent and received), and IP logs or other records of session times and durations.

The Provider is hereby ordered to disclose the above information to the government within 14 days of service of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence and instrumentalities of violations of 18 U.S.C. § 245 and 18 U.S.C. § 875(c), and occurring after November 1, 2020, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

A. Records and information relating to VICTIM-1, VICTIM-1's personal email address, and/or the Election Commission of the City of Milwaukee, Wisconsin, including any communications with associates, organizations, or others that may contain VICTIM-1's personal information and/or referencing VICTIM-1;

B. Records and information relating threats, harassment, or intimidation by the subscriber, and/or targets or potential targets of threats, harassment, or intimidation by the subscriber;

C. The identity of the person(s) who created or used the Account, including records that help reveal the whereabouts of such person(s);

D. Evidence indicating how and when the Account was accessed or used, to determine the chronological and geographic context of Account access, use and events relating to the crime under investigation and the Account subscriber;

E. Any records pertaining to the means and source of payment for services (including any credit card or bank account number or digital money transfer account information);

F. Evidence indicating the subscriber's state of mind as it relates to the crime under investigation; and

G. Evidence that may identify any co-conspirators or aiders and abettors, including records that help reveal their whereabouts.

This warrant authorizes a review of electronically stored information, communications, and other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.